Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-44 are pending in the application, with 1, 21, 34, 35, and 36 being the independent claims. Claims 1, 2, 5-9, 12, 14, 21, 28, 34-36, 40-42, and 44 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 1-35

In the Final Office Action dated April 28, 2008 ("Final Office Action"), the Examiner rejected claims 1-35 under 35 U.S.C. § 103(a) as being allegedly obvious over U.S. Patent No. 6,339,423 to Sampson et al. ("Sampson") in view of U.S. Patent No. 5,502,766 to Boebert et al. ("Boebert"), and further in view of U.S. Patent No. 6,892,306 to En-Seung et al. ("En-Seung"). In the Advisory Action dated July 16, 2008 ("Advisory Action"), the Examiner maintained this rejection. For the reasons set forth below, Applicants respectfully submit that the Examiner has failed to establish a *prima facie* case of obviousness of claims 1-35 based on the combination of Sampson, Boebert, and En-Seung.

Independent claims 1, 21, 34, and 35 each recite, *e.g.*, the step of "upon successful authentication ... retrieving at the first server machine a user key permitting

access to an encrypted header of the secured item, the encrypted header including access rules for the secured item."

The Examiner concedes that Sampson and Boebert do not teach or suggest the above-recited feature, but rather relies on En-Seung to allegedly teach this above-recited feature. (Final Office Action, p. 6). The Examiner cites to FIG. 19 and col. 3, ll. 14-32 of En-Seung in support of this position. However, En-Seung neither in this section nor anywhere else teaches or suggests an "encrypted header including access rules" as recited in claims 1, 21, 34, and 35. Instead, En-Seung teaches the use of "key information" to generate a "user key," which in turn is used to generate a "temporary validation key" for encrypting and decrypting a "copyright protection protocol format." (En-Seung, col. 3, ll. 14-32; col. 4, l. 52 - col. 5, l. 43). None of the aforementioned elements of En-Seung can reasonably be understood by a skilled artisan as being "access rules" as recited in claims 1, 21, 34, and 35.

Moreover, while En-Seung may disclose the step of "generat[ing] user authorization information," this step cannot reasonably be understood by a skilled artisan as relating to the "access rules," recited in claims 1, 21, 34, and 35. (En-Seung, FIG. 19, S230). This is because in En-Seung, this "user authorization information" refers to "encryption key information." (En-Seung, col. 15, ll. 13-16). Encryption key information is "information that is generated in the host server in response to the request of the service server when the user to be provided with the digital information is found to be unregistered with the host server." (En-Seung, col. 4, ll. 52-55; FIG. 20). This encryption key information is "used to generate a temporary validation key," and is "preferably generated by using random numbers." (En-Seung, col. 4, ll. 61-67).

Additionally, En-Seung describes the process of generating a header, as shown in FIG. 19 of En-Seung, but it is again for the purpose of encryption, as it "includes information necessary for encryption of the digital content." (En-Seung, col. 14, ll. 61-64). Accordingly, a skilled artisan would not understand the "user authorization information" of En-Seung to be "access rules" as recited in claims 1, 21, 34, and 35.

In the Advisory Action, the Examiner states:

> As recited in part, user's authorization information indicates a hash value for the user key and only when the user is determined to have the same hash value for the user's key as the hash of the user's key from the authorization information, the user is considered to be authorized. Therefore, the requirement of matching the hash is what examiner is interpreting as an "access rule" because this information dictates if the user is authorized to have access or not. (Advisory Action, p. 4).

Applicants respectfully disagree that this feature of En-Seung can reasonably be characterized as an "access ***rule***," as recited in claims 1, 21, 34, and 35. En-Seung teaches generating key information, which is sent to a user's terminal and a copy stored at the host server. (En-Seung, col. 4, ll. 52-67). The user's key is generated using this key information, and used to decrypt a temporary validation key in a data header, which in turn is used to decrypt the body of digital content. (En-Seung, col. 5, ll. 6-28). The Examiner incorrectly equates the user's ability (or inability), based on permissions associated with the user's key information, to decrypt the temporary validation key as the "access rule" recited in claims 1, 21, 34, and 35. (Advisory Action, p. 4).

However, En-Seung does not actually contain an "access rule" in the header, merely the temporary validation key. While the user's ability to use this temporary validation key to decrypt the body of digital content depends on the user's ability to decrypt the temporary validation key based on generating a matching user key with the

user's key information, the temporary validation key itself is not an "access rule," as recited in claims 1, 21, 34, and 35, but rather just a means to gain access. The rule for granting access in En-Seung, specifically that the temporary validation key be decrypted by the user having matching key information, and therefore the ability to generate the correct user's key for decrypting the temporary validation key, is not itself located in the header of En-Seung, and is simply a predetermined function.

Accordingly, although En-Seung teaches an encrypted temporary validation key in a header for providing ***access*** to authorized users through successful decryption of the temporary validation key, it cannot be said that En-Seung teaches "encrypted header including access ***rules*** for the secured item," as recited in claims 1, 21, 34, and 35.

Therefore, as En-Seung fails to cure the deficiencies of Sampson and Boebert, Sampson, Boebert, and En-Seung cannot be used to establish a prima facie case of obviousness for claims 1, 21, 34, and 35.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claims 1, 21, 34, and 35, and find them allowable over the combination of Sampson, Boebert, and En-Seung. Also, at least based on their respective dependencies, claims 2-20 and 22-33 should be found allowable over the combination of Sampson, Boebert, and En-Seung for at least the aforementioned reasons, and further in view of their own respective features.

Claim 36

In the Final Office Action, the Examiner rejected claim 36 under 35 U.S.C. § 103(a) as being allegedly obvious over Stallings (Cryptography and Network Security) in view of Narasimhalu. For the reasons set forth below, Applicants respectfully submit

that the Examiner has failed to establish a *prima facie* case of obviousness of claim 36 based on the combination of Stallings and Narasimhalu.

Claim 36 recites, in part, that "based on information stored in an encrypted header of a secure item, a given requestor ... is only permitted to access the secure item through at most one of said local servers at a time."

The Examiner states at page 4 of the Final Office Action that page 336 of the Stallings reference teaches, through the use of "session keys," accessing a secured item through at most one local server at a time, as recited in claim 36. However, the Examiner concedes Stallings does not teach or suggest "permitting access based on information stored in an encrypted header of a secure item," as recited in claim 36. (Final Office Action, p. 4). Rather, the Examiner relies on Narasimhalu as allegedly teaching the use of a secret key to encrypt a secure item, and then storing the secret key in an encrypted header, which is then used to permit access, as recited in claim 36. (Final Office Action, p. 4).

However, the Examiner's characterization of the limitation of Stallings' teachings is incomplete. Since Stallings does not teach or suggest "permitting access based on information stored in an encrypted header of a secure item," as recited in claim 36, as the Examiner concedes, Stallings also cannot teach or suggest "wherein, based on information stored in an encrypted header of a secure item a given requestor ... is only able to access the secure item using only a single one of said local servers or the central server," as recited in claim 36. Therefore, even assuming, *arguendo*, that Stallings limits access to a secured item through at most one local server at a time, and further assuming, *arguendo*, that Narasimhalu teaches permitting access based on an encrypted header,

there is no teaching or suggestion in either applied reference of "a given requestor [being] only able to access the secure item using only a single one of said local servers or the central server" where this access restriction is "based on information stored in an encrypted header of a secure item," as recited in claim 36.

In the Advisory Action, the Examiner states:

> However, Narasimhalu clearly discloses wherein, based on information stored in an encrypted header of a secure item a given requestor, permitted to access the secure item (Fig. 2 and 4 in combination with page 5 lines 35-47) through one or more of a local server (See Fig. 1, numeral 10, "Information provider", secure item is provided through information provider which is interpreted as a server). (Advisory Action, p. 5).

Without acquiescing to the Examiner's statement, the Examiner's statement in the Advisory Action fails to address the above arguments. Specifically, there is no teaching or suggestion in Stallings or Narasimhalu of allowing a given requestor to only access a secure item "using only a single one of said local servers or the central server," wherein this restriction on access is based on information in the header, as recited in claim 36. Even if Narasimhalu does teach, *arguendo*, permitting access through one or more servers based on information in an encrypted header, as the Examiner alleges in the Advisory Action on page 5, and which Applicants do not acquiesce to, this does not further imply that the header also contains information for restricting access to "only a single one" of the servers, as recited in claim 36.

For at least these reasons, the applied references cannot be used to establish a prima facie case of obviousness for independent claim 36.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claim 36 allowable over the applied reference.

Claims 37-42

The Examiner has rejected claims 37-42 under 35 U.S.C. § 103(a) as being allegedly obvious over Stallings in view of Narasimhalu, and further in view of U.S. Patent No. 6,317,777 to Skarbo et al. ("Skarbo"). Applicants respectfully traverse this rejection.

As noted above with regard to independent claim 36, the combination of Stallings and Narasimhalu do not teach or suggest that "based on information stored in an encrypted header of a secure item, a given requestor ... is only permitted to access the secure item through at most one of said local servers at a time," as recited in claim 36. At page 19 of the Final Office Action, Skarbo is used to allegedly teach an access control system coupled to an enterprise network to restrict access to secured files stored therein. Even assuming this interpretation is correct, which Applicants do not acquiesce to, Skarbo is not used to teach or suggest the above-recited distinguishing feature of claim 36, and therefore Skarbo does not cure the deficiencies of the other applied references. For at least these reasons, independent claim 36 is not rendered obvious by the combination of Stallings, Narasimhalu, and Skarbo.

Claims 37-42 depend from claim 36 and are therefore not rendered obvious by the combination of Stallings, Narasimhalu, and Skarbo for at least the aforementioned reasons for independent claim 36, and further in view of their own respective features.

Claims 43 and 44

The Examiner has rejected claims 43 and 44 under 35 U.S.C. § 103(a) as being allegedly obvious over Stallings in view of Narasimhalu, and in further view of Skarbo

as applied to claim 37, and further in view of U.S. Patent No. 6,449,721 to Pensak ("Pensak"). Applicants respectfully traverse this rejection.

As noted above with regard to independent claim 36, the combination of Stallings, Narasimhalu, and Skarbo do not teach or suggest that "based on information stored in an encrypted header of a secure item, a given requestor ... is only permitted to access the secure item through at most one of said local servers at a time," as recited in claim 36. At page 20 of the Final Office Action, Pensak is used to allegedly teach, which Applicants do not acquiesce to, secured files are secured by encryption. However, Pensak is not used to teach or suggest the above-recited distinguishing feature of claim 36, and thus Pensak does not cure the deficiencies of the other applied references. Therefore, for at least these reasons, independent claim 36 is not rendered obvious by the combination of Stallings, Narasimhalu, Skarbo, and Pensak.

Claims 43 and 44 depend from claim 36 and are therefore not rendered obvious by the combination of Stallings, Narasimhalu, Skarbo, and Pensak for at least the aforementioned reasons for independent claim 36, and further in view of their own respective features.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Final Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Jason D. Eisenberg
Attorney for Applicant
Registration No. 43,447

Date: 8/27/08

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
863976_1.DOC